УДК 004.56.5(043.2)

**О.М. Дрєєв**[1]
*Кіровоградський національний технічний університет*

# Використання методів екстраполяції часових рядів для виявлення аномальної поведінки трафіку в телекомунікаційній системі або мережі

*Вступ.* Для захисту серверів в телекомунікаційних мережах використовують багато засобів. Одним з них є виявлення відхилень параметрів трафіку від середньостатистичних. На жаль, в процесі використання мережевих ресурсів навантаження на мережу є не постійним і змінюється в досить широких межах. Тому такий метод виявляє лише досить сильні відхилення від норми. Робота розглядає можливість використання передбачення змін параметрів трафіку для порівняння з реальним процесом, на основі чого робиться висновок про ймовірність роботи системи не в штатному режимі.

*Основна частина.* Дослідження трафіку ігрового серверу виявило нестабільну періодичність навантаження мережі. На графіках спостерігалися стійкі годинні, добові та тижневі коливання з досить сильними нестабільними амплітудами. Такий сигнал можна представити як ергодичний квазіперіодичний, й проводити його апроксимацію коливними базисними функціями з некратними частотами з подальшою екстраполяцією на невеликий період часу. Прогнозування за таким тригонометричним поліномом зберігає властивості сигналу поза проміжком апроксимації, тому екстраполяція є коректною.

Проведено теоретичне оцінювання похибки прогнозування на основі узагального ряду Тейлора, де за базові функції приймаються частинні розв'язки обраного диференціального рівняння. Таке прогнозування є менш інформативним для поставленої задачі, ніж статистичне оцінювання. Тому, також проведене теоретичне оцінювання похибок прогнозування, і на основі статистичних відомостей побудовані ймовірнісні інтервали, за якими можна оцінити шлях реального процесу зміни інтенсивності трафіку з заданою надійністю дотримання меж. В разі порушення широких меж з високою надійністю, наприклад 90%, ми можемо звернути увагу адміністратора, що ймовірна мережева атака.

*Висновки.* Отримано нову систему передбачення змін обсягу трафіку на основі тригонометричних рядів з некратними частотами. Зроблено оцінку похибок передбачення на основі статистики апроксимаційних відхилень. Використано прогнозування для порівняння прогнозованого обсягу трафіку з фактичним, що дозволило виявляти ймовірні мережеві атаки на серверне обладнання. Система працює для достатньої кількості клієнтів, для яких можливо використовувати методи статистичної математики.

---

[1] асистент кафедри програмного забезпечення